



125051, г. Москва, ул. Семеновская Б., д.45  
тел. +7 495 730-74-88 <http://www.inforion.ru>

## **Комментарии**

к Положению о методах и способах защиты информации  
в информационных системах персональных данных,  
утверждённому приказом ФСТЭК России от 5 февраля 2010 г. №58

*А.В. Кузнецов, ведущий эксперт отдела проектных работ ООО «ИНФОРИОН»*

г. Москва, 2010 г.

## Общие сведения

Анализируя события последних месяцев, можно сделать вывод о том, что на сегодняшний день совершенствование законодательства в области обработки и обеспечения безопасности персональных данных представляет собой итерационный процесс.

В 2008 году Федеральная служба по техническому и экспортному контролю (ФСТЭК России) выпустила в соответствии с «Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденным постановлением Правительства РФ от 17 ноября 2007 г. № 781, четыре методических документа (МД), получивших в кругу специалистов условное наименование «четверокнижие»:

1. Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных, утверждены заместителем директора ФСТЭК России 15.02.2008 г.
2. Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утверждены заместителем директора ФСТЭК России 15.02.2008 г.
3. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена заместителем директора ФСТЭК России 15.02.2008 г.
4. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена заместителем директора ФСТЭК России 14.02.2008 г.

Данные документы не были предоставлены широкой публике (т.е. всем операторам персональных данных), так как имели пометку «для служебного пользования» и предоставлялись только по специальному запросу. Но даже у получивших их организаций (в большинстве своем это были лицензиаты ФСТЭК России) возникали многочисленные вопросы относительно статуса документов и их содержанию:

1. Документы утверждены заместителем директора, а не самим директором ФСТЭК России.
2. Документы не зарегистрированы в Министерстве юстиции РФ, но при этом объявлено, что они содержат обязательные для всех операторов требования по обеспечению безопасности персональных данных (ПДн).

3. Документы существуют в двух (по некоторым данным – в трех) незначительно отличающихся редакциях.
4. Документы взаимно не согласованы, содержат смысловые, синтаксические и орфографические ошибки.

После многочисленных запросов, дискуссий, конференций и семинаров осенью 2009 года в виде выписок с рядом поправок «четверокнижие» появляется на официальном сайте ФСТЭК России, чуть позже пометка «для служебного пользования» снимается решением ФСТЭК России от 16 ноября 2009 г., но внесенные изменения не переутверждаются и «обновляемые» таким образом документы считаются действующими с февраля 2008 года.

В конце 2009 года Федеральным законом от 27 декабря 2009 года № 363-ФЗ внесены изменения в Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных», которые устанавливают «второе пришествие» 1 января 2011 года и исключают требование по обязательному использованию криптографических средств для защиты персональных данных<sup>1</sup>. При этом ряд обсуждаемых альтернативных законопроектов и комплексных поправок в федеральное законодательство (в том числе в ФЗ от 8 августа 2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности») не принимается.

В конце февраля 2010 года (спустя два года с начала активной «эпопеи» в области защиты персональных данных) в сети Интернет появляется проект документа «Положение о методах и способах защиты информации в информационных системах персональных данных», который открывает новые перспективы для операторов, выбравших выжидательную позицию и заставляет задуматься операторов, выполнивших мероприятия в ранее установленный срок (до 1 января 2010 года), о целесообразности своих действий.

В марте 2010 года данный документ размещается в информационно-справочных системах с пометкой «недействующий», но он уже утвержден приказом директора ФСТЭК России от 5 февраля 2010 №58 и зарегистрирован в Минюсте России 19 февраля 2010 г. за № 16456. Совсем скоро Положение вступает в силу (публикуется в Российской газете 5 марта 2010 г., № 46).

Регистрация в Минюсте России и утверждение директором ФСТЭК России (т.е. «первым лицом») показывает определенную «работу над ошибками», проделанную ФСТЭК России в области организации деятельности по подготовке нормативно-правовых актов.

---

<sup>1</sup> Следует отметить, что даже до внесения изменений в ст. 19 Федерального закона «О персональных данных» применение криптографической защиты осуществлялось только в случае определения оператором необходимости обеспечения безопасности ПДн с использованием криптосредств, а также при обеспечении безопасности ПДн при обработке в информационных системах, отнесенных к компетенции ФСБ России

С выходом Положения возник вопрос о статусе «четверокнижия». Следует отдать должное ФСТЭК России: практически сразу было принято решение от 5 марта 2010 г. не применять с 15 марта 2010 г. для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных следующие методические документы ФСТЭК России:

1. Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных, утвержденные заместителем директора ФСТЭК России 15 февраля 2008 г.;
2. Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные заместителем директора ФСТЭК России 15 февраля 2008 г.

Ниже будут рассмотрены и прокомментированы основные статьи Положения<sup>2</sup> о методах и способах защиты информации в информационных системах персональных данных.

Следует отметить, что никаких принципиальных изменений в подходах и принципах обеспечения безопасности ПДн не произошло, и тем операторам, которые потратили средства, время и силы на реализацию мероприятий предусмотренных «четверокнижием», не стоит огорчаться.

Из одной из очевидных особенностей хочется обратить внимание на переход от понятия «обеспечения безопасности персональных данных<sup>3</sup>» к понятию «защита информации<sup>4</sup>».

Дальнейший анализ документа приведен в следующем разделе.

---

<sup>2</sup> Комментарии выделены курсивом. Дополнительно проведено сопоставление Положения с документом «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утвержденным приказом Гостехкомиссии России от 30.08.2002 г. № 282 и другими руководящими документами Гостехкомиссии (ФСТЭК) России.

<sup>3</sup> Обеспечение состояния защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность [ГОСТ Р 50922-2006]. Обеспечение состояния защищенности данных, обрабатываемых средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз [РД Защита от несанкционированного доступа к информации. Термины и определения]

<sup>4</sup> Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию [ГОСТ Р 50922-2006]

## Анализ и комментарии к Положению о методах и способах защиты информации в информационных системах персональных данных

В настоящем разделе приводятся некоторые выдержки из Положения и даются комментарии к ним. Так же обобщаются и консолидируются отдельные требования по защите информации.

1.1. Настоящее Положение устанавливает методы и способы защиты информации, применяемые для обеспечения безопасности ПДн при их обработке в информационных системах персональных данных (ИСПДн).

В настоящем Положении не рассматриваются:

- вопросы обеспечения безопасности персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну;
- вопросы применения криптографических методов и способов защиты информации.

1.2. К методам и способам защиты информации в информационных системах относятся:

- методы и способы защиты информации, обрабатываемой техническими средствами информационной системы, от несанкционированного, в том числе, случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий (далее - методы и способы защиты информации от несанкционированного доступа);

- методы и способы защиты речевой информации, а также информации, представленной в виде информативных электрических сигналов, физических полей, от несанкционированного доступа к ПДн, результатом которого может стать копирование, распространение персональных данных, а также иных несанкционированных действий (далее - методы и способы защиты информации от утечки по техническим каналам).

*Положение определяет два основных направления защиты ПДн – направление нейтрализации угроз, реализуемых за счет несанкционированного доступа и направление нейтрализации угроз, реализуемых за счет утечки по техническим каналам (согласуется с п. 5.1.2. СТР-К).*

*Таким образом, данное Положение не отменяет защиту от утечки информации по техническим каналам для ИСПДн, хотя многие операторы этого ожидали. При этом надо понимать, что такие мероприятия необходимы только в том случае, если эти угрозы актуальны для конкретной ИСПДн.*

1.3. Для выбора и реализации методов и способов защиты информации в информационной системе оператором или уполномоченным лицом может назначаться структурное подразделение или должностное лицо (работник), ответственные за обеспечение безопасности персональных данных.

Для выбора и реализации методов и способов защиты информации в информационной системе может привлекаться организация, имеющая оформленную в установленном порядке лицензию на осуществление деятельности по технической защите конфиденциальной информации.

*В данном пункте произошла важная коррекция положений предыдущих документов: во-первых «должен назначаться ответственный» заменено на – «может», во-вторых, четко прописана возможность привлечения лицензиатов для выполнения работ связанных с обеспечением безопасности ПДн (согласуется с п. 2.15., 3.4. СТР-К). Раньше данная возможность была явно прописана только в МД ФСБ России.*

*Для многих операторов остается открытым вопрос о необходимости лицензирования деятельности по технической защите конфиденциальной информации (ТЗКИ).*

*Ранее в отмененных «Основных мероприятиях ...» (п. 3.14.) была указана необходимость получения оператором лицензии на деятельность по ТЗКИ в зависимости от класса его ИСПДн и ее распределенности. В Положении такая необходимость явно не прописана.*

*Однако в данном вопросе определяющим является Федеральный закон от 8 августа 2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности», согласно статье 17 которого деятельность по технической защите конфиденциальной информации подлежит обязательному лицензированию в порядке и на условиях, определяемых Положением о лицензировании деятельности по технической защите конфиденциальной информации.*

*Таким образом, если оператор собирается самостоятельно осуществлять технические мероприятия по защите ПДн, то он должен получить соответствующую лицензию.*

*Часто возникает мнение, что в случае осуществления технических мероприятия для обеспечения собственных нужд получать данную лицензию не нужно. Это мнение не совсем верно по двум причинам:*

*- Федеральный закон «О лицензировании отдельных видов деятельности» для подобных случаев предусматривает указание в скобках после наименования лицензируемого вида деятельности формулировки «за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя»; для деятельности по ТЗКИ такого специального указания нет;*

*- Положение о лицензировании деятельности по технической защите конфиденциальной информации определяет, что под технической защитой конфиденциальной информации понимается комплекс мероприятий и (или) услуг по ее защите, т.е. не только услуги (деятельность «на продажу»).*

1.4. Выбор и реализация методов и способов защиты информации в информационной системе осуществляются на основе определяемых оператором (уполномоченным лицом) угроз безопасности персональных данных (модели угроз) и в зависимости от класса информационной системы, определенного в соответствии с Порядком проведения классификации информационных систем персональных данных, утвержденным приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20 (зарегистрирован Минюстом России 3 апреля 2008 г., регистрационный № 11462)<sup>5</sup>. Модель угроз разрабатывается на основе методических документов, утвержденных в соответствии с пунктом 2 постановления Правительства Российской Федерации от 17 ноября 2007 г. № 781.

*Положения данного пункта вернули нас к первоначальным подходам к проведению классификации ИСПДн, т.е. класс специальных ИСПДн в соответствии с п. 16 совместного приказа ФСТЭК/ФСБ/Мининформсвязи России определяется на основе модели угроз исходя из оценки возможного ущерба (до этого осенние изменения в документе «Рекомендации ...» предусматривали, что класс любой информационной системы определяется в соответствии с таблицей (по  $X_{нпд}$  и  $X_{пд}$ )).*

*Подход к классификации на основе оценки ущерба был прокомментирован заместителем начальника управления ФСТЭК России, начальником отдела управления ФСТЭК России и главным научным сотрудником ГНИИ ПТЗИ ФСТЭК России в статье «Обработка персональных данных в информационных системах: как обеспечить безопасность» журнала CONNECT в январе 2009 года.*

*В основе данного подхода лежат сопоставление определения классов типовых ИСПДн в соответствии с совместным приказом ФСТЭК/ФСБ/Мининформсвязи России:*

*класс 1 (К1)- ИСПДн, для которых нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных;*

*класс 2 (К2) - ИСПДн, для которых нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных;*

*класс 3 (К3) - ИСПДн, для которых нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных;*

*класс 4 (К4) - ИСПДн, для которых нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных.*

<sup>5</sup> Получил в средствах массовой информации определение «тройного» приказа

и определения показателя опасности угрозы (МД ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»):

*низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;*

*средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;*

*высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.*

*Основным плюсом данного подхода является его гибкость, он позволяет наиболее адекватно обосновать выбор класса для ИСПДн, не основываясь только на количестве и категории ПДн.*

*Надо также отметить, что построение модели угроз осуществляется для всех типов ИСПДн (типовые и специальные), а не только для специальных ИСПДн<sup>6</sup>.*

2.1. Методами и способами защиты информации от несанкционированного доступа являются:

- реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;
- ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также, хранятся носители информации;
- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
- регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;
- учет и хранение съемных носителей информации и их обращение, исключаящее хищение, подмену и уничтожение;
- резервирование технических средств, дублирование массивов и носителей информации;
- использование средств защиты информации (СрЗИ), прошедших в установленном порядке процедуру оценки соответствия;
- использование защищенных каналов связи;
- размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;
- организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;

<sup>6</sup> *Изначально это было предусмотрено п. 12 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных утвержденного Постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781*

- предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

*Данный перечень по большей части построен на основных рекомендуемых мерах защиты информации, приведенных в п 5.1.3. СТР-К, т.е. преемственность принципов и подходов, заложенных в основу защиты информации с ограниченным доступом, не содержащей сведений составляющих государственную тайну (конфиденциальной информации), сохраняется.*

*В перечне методов и способов защиты информации от НСД хотелось бы обратить внимание на использование СрЗИ, прошедших в установленном порядке процедуру оценки соответствия.*

*На сегодняшний день процедурой оценки соответствия для СрЗИ является их сертификация по требованиям безопасности информации. Под сертификацией средств защиты информации по требованиям безопасности информации понимается деятельность по подтверждению их соответствия требованиям государственных стандартов или иных нормативных документов по защите информации, утвержденных Государственной технической комиссией при Президенте Российской Федерации (ныне ФСТЭК России)<sup>7</sup>.*

*Таким образом, не отменяется требование об использовании сертифицированных СрЗИ, тем более, если ИСПДн в итоге будет проходить процедуру оценки соответствия (аттестацию).*

*Сразу хотелось бы отметить, что требования к обязательной аттестации ИСПДн в данном документе отсутствуют (ранее было предусмотрено п. 3.11. документа «Основные мероприятия ...»). Однако со своей стороны мы рекомендуем проводить аттестацию ИСПДн по требованиям безопасности информации. Аттестация по требованиям безопасности информации вызвана необходимостью официального подтверждения эффективности комплекса используемых в ИСПДн мер и средств защиты информации, она является комплексом организационно-технических мероприятий, в результате которых посредством специального документа – «Аттестата соответствия» подтверждается, что ИСПДн соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных ФСТЭК (Гостехкомиссией) России<sup>8</sup>.*

<sup>7</sup> Положение о сертификации средств защиты информации по требованиям безопасности информации, утверждено приказом председателя Государственной технической комиссии при Президенте Российской Федерации от 27 октября 1995 г. № 199

<sup>8</sup> Положение по аттестации объектов информатизации по требованиям безопасности информации, утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.

2.2. В системе защиты персональных данных информационной системы в зависимости от класса информационной системы и исходя из угроз безопасности персональных данных, структуры информационной системы, наличия межсетевого взаимодействия и режимов обработки персональных данных с использованием соответствующих методов и способов защиты информации от несанкционированного доступа реализуются функции управления доступом, регистрации и учёта, обеспечения целостности, анализа защищённости, обеспечения безопасного межсетевого взаимодействия и обнаружения вторжений. Методы и способы защиты информации от несанкционированного доступа, обеспечивающие функции управления доступом, регистрации и учёта, обеспечения целостности, анализа защищённости, обеспечения безопасного межсетевого взаимодействия в зависимости от класса информационной системы определяются оператором (уполномоченным лицом) в соответствии с приложением к настоящему Положению.

*Претерпев третье изменение наименования (в руководящих документах Гостехкомиссии России это были «подсистемы», в «четверокнижие» – «мероприятия», теперь – «функции») мы имеем то же самое деление требований на группы:*

- *управление доступом;*
  - *регистрация и учёт;*
  - *обеспечение целостности;*
  - *анализ защищённости;*
  - *обеспечение безопасного межсетевого взаимодействия;*
  - *обнаружение вторжений.*
- Подсистемы предусмотренные РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»*

2.3. В информационных системах, имеющих подключение к информационно-телекоммуникационным сетям международного информационного обмена (сетям связи общего пользования), или при функционировании которых предусмотрено использование съемных носителей информации, используются средства антивирусной защиты.

*Из анализа пункта 2.3 видно, что в Положении отдельно определены случаи использования антивирусных средств. Это логично: например если в качестве ИСПДн используется автономный ПК, в который осуществляется только ручной ввод информацию (без использования съемных носителей), а выводятся ПДн только на локальный принтер, то актуальность применения антивирусных средств находится под вопросом.*

*В дальнейшей части документа произошли более интересные изменения, видна более детальная проработка вопросов межсетевого взаимодействия ИСПДн. Теперь выделяются несколько типов таких взаимодействий, к которым наряду с методами и способами*

указанными выше, добавляются еще так называемые «основные методы и способы» для данного взаимодействия.

Ниже приведена таблица для разных типов межсетевого взаимодействия ИСПДн с указанием «основных методов и способов» защиты информации.

<b>Тип взаимодействия</b>					
<b>Наименование основных методов и способов защиты информации</b>	ИСПДн + сеть общего пользования	ИСПДн + сеть общего пользования с целью получения общедоступной информации	При удаленном доступе к ИСПДн через сеть общего пользования	При межсетевом взаимодействии отдельных ИСПДн через сеть общего пользования	При межсетевом взаимодействии отдельных ИСПДн разных операторов через сеть общего пользования
Межсетевое экранирование	+	+	+	+	+
Обнаружение вторжений	+	+	+	+	+
Анализ защищенности (сканеры безопасности)	+	+	+	+	+
Защита информации при ее передаче по каналам связи	+	+	+	+	+
Использование средств для надежной идентификации и аутентификации пользователей	+	+	+	+	+
Использование средств антивирусной защиты	+	+	+	+	+
Централизованное управление СЗПДн	+	+	+	+	+
Фильтрация входящих (исходящих) сетевых пакетов по правилам		+			
Периодический анализ (имитация внешних атак)		+			
Активный аудит безопасности		+			
Анализ принимаемой информации, в том числе на наличие вирусов		+			
Проверка подлинности отправителя и целостности данных			+	+	+
Управление доступом к ПДн			+		
Использование атрибутов безопасности			+		
Создание канала связи, обеспечивающего защиту передаваемой информации				+	+
Осуществление аутентификации взаимодействующих информационных систем				+	+
Обеспечение предотвращения возможности отрицания пользователем факта отправки/получения ПДн					+

*Остановимся на некоторых «основных методах и способах» защиты информации более подробно.*

- межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы

*Вопрос вызывает трансляция сетевых адресов (Network Address Translation, NAT), данный функционал предусмотрен для межсетевых экранов 2 класса защищенности (п. 2.5.1. РД Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»), но рассматриваемый механизм реализуется практически любым маршрутизирующим устройством и зачастую уже существует в вычислительных сетях оператора. Исходя из того, что требования к межсетевым экранам будут приведены ниже, считаем возможным реализацию данного механизма другими (в том числе несертифицированными) средствами.*

- периодический анализ безопасности установленных межсетевых экранов на основе имитации внешних атак на информационные системы

*Судя по всему, предлагается периодически осуществлять тесты на проникновение (ethical hacking, penetration test), но утвержденных методик для данных мероприятий на сегодняшний день нет, поэтому мы рекомендуем целесообразность данного мероприятия определять исходя из заданных ограничений на финансовые, материальные, трудовые и временные ресурсы, а при его планировании и проведении пользоваться Best Practices отрасли информационной безопасности.*

- проверка подлинности отправителя (удаленного пользователя) и целостности передаваемых по информационно-телекоммуникационной сети международного информационного обмена (сети связи общего пользования) данных;

- обеспечение предотвращения возможности отрицания пользователем факта отправки персональных данных другому пользователю;

- осуществление аутентификации взаимодействующих информационных систем и проверка подлинности пользователей и целостности передаваемых данных

*Данные мероприятия можно реализовать например за счет применения электронной цифровой подписи<sup>9</sup>.*

- использование атрибутов безопасности

*Атрибут безопасности – информация, связанная с субъектами, пользователями и/или объектами, которая используется для осуществления политики безопасности объекта оценки (п. 2.3. РД Гостехкомиссии России «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий»).*

*С атрибутами безопасности (такими как идентификатор, группы, роли, уровни безопасности или целостности) осуществляется ассоциация пользователей при идентификации и аутентификации.*

*Однозначная идентификация пользователей и правильная ассоциация атрибутов безопасности с пользователями и субъектами критичны для осуществления принятых политик безопасности.*

- обеспечение предотвращения возможности отрицания пользователем факта получения персональных данных от другого пользователя

*Для случая использования в качестве средств получения ПДн почтовых клиентов с встроенной ЭЦП возможна организация «подписанного» автоответа. Для остальных случаев это достигается внесением изменений в технологический процесс обработки ПДн (в прикладное программное обеспечение и пр.). Данное мероприятие практически не может быть обеспечено организационными мерами и представляется достаточно проблематичным при реализации.*

2.5 Подключение информационных систем, обрабатывающих государственные информационные ресурсы, к информационно-телекоммуникационным сетям международного информационного обмена осуществляется в соответствии с Указом Президента Российской Федерации от 17 марта 2008 г. N 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

<sup>9</sup> ЭЦП – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе (ФЗ от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи»)

Отметим основные положения указа № 351:

а) подключение информационных систем, ..., применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну, либо информации, обладателями которой являются государственные органы и которая содержит сведения, составляющие служебную тайну, к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу Российской Федерации, в том числе к международной компьютерной сети "Интернет" (далее - информационно-телекоммуникационные сети международного информационного обмена), не допускается;

б) при необходимости подключения информационных систем, ..., указанных в подпункте "а" настоящего пункта, к информационно-телекоммуникационным сетям международного информационного обмена такое подключение производится только с использованием специально предназначенных для этого средств защиты информации, в том числе шифровальных (криптографических) средств, прошедших в установленном законодательством Российской Федерации порядке сертификацию в Федеральной службе безопасности Российской Федерации и (или) получивших подтверждение соответствия в Федеральной службе по техническому и экспортному контролю. Выполнение данного требования является обязательным для операторов информационных систем, владельцев информационно-телекоммуникационных сетей и (или) средств вычислительной техники;

в) государственные органы в целях защиты общедоступной информации, размещаемой в информационно-телекоммуникационных сетях международного информационного обмена, используют только средства защиты информации, прошедшие в установленном законодательством Российской Федерации порядке сертификацию в Федеральной службе безопасности Российской Федерации и (или) получившие подтверждение соответствия в Федеральной службе по техническому и экспортному контролю.

Важно отметить, что подключение ИСПДн к ИСПДн другого класса или к сети связи общего пользования в любом случае осуществляется с использованием межсетевых экранов.

2.12. Программное обеспечение средств защиты информации, применяемых в информационных системах 1 класса, проходит контроль отсутствия недекларированных возможностей. Необходимость проведения контроля отсутствия недекларированных возможностей программного обеспечения средств защиты информации, применяемых в информационных системах 2 и 3 классов, определяется оператором (уполномоченным лицом).

*Данный пункт вносит ясность в необходимость сертификации по уровню контроля отсутствия недеklarированных возможностей. До этого «Основные мероприятия ...» предусматривали, что в ИСПДн должен проводиться контроль на наличие недеklarированных возможностей в программном и программно-аппаратном обеспечении, что создавало для операторов определенные трудности в трактовке и реализации этого требования.*

*Теперь все приведено в соответствии с РД Гостехкомиссии России «Защита от несанкционированного доступа. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей» и касается только СрЗИ. При этом в приложении к Положению (п. 7) уточняется соответствие 4 уровню контроля отсутствия недеklarированных возможностей.*

2.13. В зависимости от особенностей обработки персональных данных и структуры информационных систем могут разрабатываться и применяться другие методы защиты информации от несанкционированного доступа, обеспечивающие нейтрализацию угроз безопасности персональных данных.

*Данный пункт дает определённую свободу действий при построении системы защиты. Мы со своей стороны советуем придерживаться классического подхода к составу подсистем СЗПДн (подсистемы управления доступом, регистрации и учета и т.д.) и к порядку построения СЗПДн (предпроектная стадия, проектирование, ввод в действие<sup>10</sup>), так как данный подход является устоявшимся и упрощает проверяющим процесс контроля выполнения требований.*

3.1. Защита речевой информации и информации, представленной в виде информативных электрических сигналов и физических полей, осуществляется в случаях, когда при определении угроз безопасности персональных данных и формировании модели угроз применительно к информационной системе являются актуальными угрозы утечки акустической речевой информации, угрозы утечки видовой информации и угрозы утечки информации по каналам побочных электромагнитных излучений и наводок, определенные на основе методических документов, утвержденных в соответствии с пунктом 2 постановления Правительства Российской Федерации от 17 ноября 2007 г. № 781.

*Необходимо подчеркнуть, что защита информации от утечки по техническим каналам осуществляется только в случае ее необходимости (определяется моделью угроз).*

*Детально данные вопросы в настоящем документе не рассматриваются, так как требуют достаточно подробного изложения.*

<sup>10</sup> Стадии создания автоматизированных систем предусмотрены ГОСТ 34.601-90, ГОСТ Р 51583-2000 и СТР-К



125051, г. Москва, ул. Семеновская Б., д.45  
тел. +7 495 730-74-88 <http://www.inforion.ru>

*Требования к защите от несанкционированного доступа в зависимости от класса информационной системы приведены в приложении к Положению.*

*Для простоты восприятия далее будет приведена сводная таблица для ИСПДн различного класса и таблица их сопоставление с классами защищенности автоматизированных систем в части касающейся.*



125051, г. Москва, ул. Семеновская Б., д.45  
 тел. +7 495 730-74-88 http://www.inforion.ru

Наименование требований	Класс ИСПДн									
	4	3_1	2_1	1_1	Равные права			Разные права		
					3_N	2_N	1_N	3_N	2_N	1_N
<b>Управление доступом</b>	По решению оператора									
Идентификация, проверка подлинности и контроль доступа субъектов:										
в систему		+	=	+	+	=	+	+	=	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ							+			+
к программам							+			+
к томам, каталогам, файлам, записям, полям записей							+			+
Контроль доступа в соответствии с матрицей доступа										+
<b>Регистрация и учет</b>										
Регистрация и учет:										
входа (выхода) субъектов доступа в (из) систему (узел сети)		+	=	+	+	=	+	+	=	+
выдачи печатных (графических) выходных документов				+			+			+
запуска (завершения) программ и процессов (заданий, задач)							+			+
доступа программ субъектов доступа к защищаемым файлам							+			+
доступа программ субъектов доступа к дополнительным защищаемым объектам (терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей)							+			+
Учет носителей информации / дублирующий учет		+/-	=	+ / +	+/-	=	+ / +	+/-	=	+ / -
Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей				+			+			+
<b>Обеспечение целостности</b>										
Обеспечение целостности программных средств и обрабатываемой информации		+	=	+	+	=	+	+	=	+
Физическая охрана средств вычислительной техники и носителей информации		+	=	+	+	=	+	+	=	+
Периодическое тестирование СЗИ НСД		+	=	+	+	=	+	+	=	+
Наличие средств восстановления СЗИ НСД	+	=	+	+	=	+	+	=	+	

Условные обозначения:

«\_1» - однопользовательский режим обработки ПДн

«\_N» - многопользовательский режим обработки ПДн

«=» - соответствуют требованиям к более низкому классу ИСПДн



125051, г. Москва, ул. Семеновская Б., д.45  
тел/факс +7 495 730-74-88

<http://www.inforion.ru>

Наименование подсистемы	Класс ИСПДн									
	4	3_1	2_1	1_1	Равные права			Разные права		
					3_N	2_N	1_N	3_N	2_N	1_N
Управление доступом		ЗБ	ЗБ	ЗА	2Б	2Б	2А*	1Д	1Д	1Г
Регистрация и учет		ЗБ	ЗБ	ЗА	2Б	2Б	2А*	1Д	1Д	1Г
Обеспечение целостности		ЗБ	ЗБ	ЗА	2Б	2Б	2А*	1Д	1Д	1Г

\* - Для автоматизированных систем, имеющих класс защищенности 2А РД Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» предусмотрена криптографическая подсистема.

Необходимо отметить, что для всех классов ИСПДн с разными правами доступа к ПДн целостность СЗПДн проверяется при загрузке системы по контрольным суммам компонентов системы защиты (не по наличию имен (идентификаторов) её компонент).

Требования к межсетевым экранам (МЭ) для ИСПДн различных классов приведены в таблице.

Наименование требований	Класс ИСПДн		
	3	2	1
Фильтрация на сетевом уровне для каждого сетевого пакета независимо	+	+	+
Фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств	⊕	+	+
Фильтрация с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов		+	+
Фильтрация с учетом любых значимых полей сетевых пакетов		+	+
Фильтрация на транспортном уровне запросов на установление виртуальных соединений			+
Фильтрация на прикладном уровне запросов к прикладным сервисам			+
Фильтрация с учетом даты/времени			+
Идентификация и аутентификация администратора при его локальных запросах на доступ	+	+	+
Аутентификация входящих и исходящих запросов методами, устойчивыми к пассивному и/или активному прослушиванию сети			+
Предотвращение доступа неидентифицированного субъекта или субъекта, подлинность идентификации которого при аутентификации не подтвердилась			+
Идентификация и аутентификация администратора при его удаленных запросах методами, устойчивыми к пассивному и активному перехвату информации			+
Регистрация входа (выхода) администратора межсетевого экрана в систему(из системы)	+	+	+
Регистрация и учета фильтруемых пакетов		+	+
Регистрация запуска программ и процессов (заданий, задач)		+	+
Регистрация и учет запросов на установление виртуальных соединений			+
Локальная сигнализация попыток нарушения правил фильтрации			+
Регистрация действия администратора МЭ по изменению правил фильтрации			+
Возможность дистанционного управления своими компонентами			+
Контроль целостности своей программной и информационной части	+	+	+
<i>по контрольным суммам</i>			+
Восстановление свойств межсетевого экрана после сбоев и отказов оборудования	+	+	+
Регламентное тестирование	+	+	+

Сравнение требований к МЭ, приведенных в Положении и требований, приведенных в РД Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»<sup>11</sup>, позволяет сделать выводы о следующих соответствиях:

ИСПДн 3 класса – 5 класс защищенности МЭ по РД (плюс одно требование из 4 класса);

<sup>11</sup> В Положении отсутствуют требования к документации на МЭ, существующие в соответствующем РД



125051, г. Москва, ул. Семеновская Б., д.45  
тел/факс +7 495 730-74-88

<http://www.inforion.ru>

*ИСПДн 2 класса – 4 класс защищенности МЭ по РД;*

*ИСПДн 1 класса – 3 класс защищенности МЭ по РД.*

*Отметим, что фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств для МЭ ИСПДн 3 класса с большой вероятностью попала сюда просто по ошибке.*

5. Анализ защищенности проводится для распределенных информационных систем и информационных систем, подключенных к сетям международного информационного обмена, путем использования в составе информационной системы программных или программно-аппаратных средств (систем) анализа защищенности. Средства (системы) анализа защищенности должны обеспечивать возможность выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения информационной системы, которые могут быть использованы нарушителем для реализации атаки на систему.

6. Обнаружение вторжений проводится для информационных систем, подключенных к сетям международного информационного обмена, путем использования в составе информационной системы программных или программно-аппаратных средств (систем) обнаружения вторжений.

*Требования к данным средствам применительно к классам ИСПДн не определены, таким образом, есть возможность выбора из достаточно большого списка данных средств, наиболее подходящих для конкретной ИСПДн.*

## **Заключение**

Следует отметить, что новый документ, пришедший на смену методическим документам предыдущего поколения, представляет собой более удобное руководство с точки зрения его применения. В Положении расставлено большинство (не все) точки над «і», и оно менее противоречиво по своему содержанию. Требования по защите информации более приблизились к реальной жизни и операторы теперь в большей мере способны их реализовать.